DNS Abuse Mitigation - Proactive Enforcement Framework

ICANN Contractual Compliance

29 April 2026

Agenda

Proactive DNS Abuse Mitigation Enforcement Framework

- Objective & Scope
- Selection Criteria
- Process
- Key Performance Indicators
- Discussion & Input

Objective & Scope

- **Strengthen ICANN's enforcement** of the requirements in the RAA and RAs.
  - Identify **potential noncompliance** with DNS Abuse mitigation obligations that may not surface through complaints or audits, thereby **complementing** existing **complaint-driven and audit-based processes.**

- Applies to **registrars** and **gTLD registry operators** that meet **defined data-driven criteria**, focusing attention on contracted parties where **DNS Abuse appears most concentrated** and/or is **mitigated less promptly**.

- Reviews **assess** whether contracted parties take **timely and appropriate mitigation actions** based on actionable evidence and, where they do not, examine the reasons and identify **what changes are needed** to support continued compliance.

- Launch **new proactive reviews each quarter**, each focusing on approximately **five to seven contracted parties** at a time.

How Contracted Parties Are Selected

- A **data-driven model** identifies contracted parties with elevated DNS Abuse indicators based on observations derived from:
    - **Operational DNS Abuse patterns and portfolio-level indicators**, such as concentrations of reported DNS Abuse, mitigation performance metrics, and clustered registration behaviors.
    - **Past compliance performance**, including prior enforcement actions and the effectiveness of any remediation presented.
    - **Diverse external intelligence sources**.

→**Flexible, adaptive scoring approach** that evolves as new patterns, data, and operational insights emerge.

- **Identified parties** enter the quarterly review cycle. If any are already undergoing an **enforcement action** that includes detailed DNS Abuse questions, they are skipped and the **next highest-ranked eligible party** is selected.

What Happens During a Proactive Review

- **Weeks 1–3: Preparation and Selection**
  - Collect **data** from all available sources.
  - Apply the **scoring matrix** to identify and **select contracted parties** for review.

- **Weeks 4–12: Investigation, Engagement, and Remediation**
  - ICANN Compliance **issues a notification** describing the observed indicators and the relevant contractual obligations.
  - The contracted party **submits details** on its **investigation**, mitigation actions, and **DNS Abuse handling process**.
  - ICANN Compliance **reviews responses**, requests clarification as needed, and verifies **remediation** plan implementation to facilitate continued compliance.

- All **correspondence, findings, scoring details**, and contracted party responses, including any **remediation**, **are documented** in the Naming Services portal (NSp).

Key Performance Indicators (KPIs)

- **Outcome KPIs (Effectiveness)**
  - Percentage of contracted parties reviewed each quarter.
  - Percentage of reviews that led to remediation plans involving processes and/or systems.
  - Demonstrable improvement in the DNS Abuse indicators ranking used to select reviewed contracted parties over the next two quarters.*
  - Reduction in uptime of reported abusive domains over the next two quarters.*
  *Exact % to be set after baseline is established.

- **Operational KPIs (Timeliness & Process Adherence)**
  - On-time completion of data collection, scoring, issuance of compliance notifications, and completion of investigations within the established timeframes.

- **Transparency & Reporting KPIs**
  - Quarterly publication of proactive action metrics on the ICANN Compliance dashboard. Target: Published within one month of cycle completion.

Discussion & Input

We welcome your **feedback and discussion** on:

- The overall program design, including cadence, process flow, and the categories of risk indicators used.
- Preferred levels of transparency - what information is most valuable for the ICANN community to see regarding this framework.
- Operational and implementation considerations - insights from your own experience meeting current requirements that we should factor into this approach.
- Your DNS Abuse mitigation efforts - how you are strengthening DNS Abuse mitigation today and how you are preparing for the upcoming requirements.

ICANN Webpage and Social Media Links


icann.org


@icann


facebook.com/icannorg


youtube.com/icannnews


flickr.com/icann


linkedin.com/company/icann


instagram.com/icannorg